What is claimed is:

1. A method of protecting a network from potentially harmful data traffic traversing a plurality of data ports of the network, the data traffic comprising data packets, the method comprising the steps of:

monitoring all the data packets traversing the data ports from a plurality of sources;

determining the number of data packets form each source traversing the data ports during a predetermined period of time; and

denying access to the data ports to data packets from a particular source if the number of packets traversing the ports from that source is greater than a predetermined number during the predetermined period of time.

2. The method according to claim 1 wherein the step of denying access to the source is automatic.

3. The method according to claim 1 further comprising the step of copying each of the data packets for monitoring.

4. The method according to claim 1 wherein the step of monitoring further comprises monitoring both incoming and outgoing data packets traversing the data ports.

5. The method according to claim 1 where the step of monitoring further comprises separately monitoring the data packets traversing each of the data ports.

6. The method according to claim 3 further comprising using protocol information of the copied data packets in denying access to the data ports.

7. The method according to claim 6 wherein the step of using the protocol information further comprises storing in a memory

the source addresses of the data packets traversing the data ports during the predetermined period of time.

8. The method according to claim 7 further comprising sorting the data packets traversing the data ports based upon the source addresses of each data packet.

9. The method according to claim 8 wherein the step of sorting further comprises creating a reference index having a number count for determining the number of data packets from each source traversing the data ports and incrementing the number count when subsequent data packets from the same source address traverse the data ports during the predetermined period of time.

10. The method according to claim 9 further comprising erasing from memory the reference index after the predetermined period of time expires.

11. The method according to claim 1 further comprising allowing data packets from sources other than the denied source to traverse the data ports.

12. The method according to claim 1 wherein the predetermined number of packets traversing the data ports and the predetermined period of time is configurable for each of the data ports.

13. A method of protecting a data network from data packets being sent from a suspicious source, the method comprising the steps of sampling the data packets and identifying a source that sends packets in excess of a predetermined number during a predetermined time.

14. The method according to claim 13 further comprising excluding from the data network data packets transmitted from the identified source.

15. A method of protecting a network from data packets transmitted by a suspicious source, the method comprising the steps of sampling the data packets transmitted to and from the network, identifying any source that transmits data packets to and from the network in excess of a predetermined rate, and automatically excluding from the network data packets from the identified source for a predetermined time.

16. A system for protecting a network, the system comprising a monitoring means programmed for sampling data packets transmitted to and from the network, a memory for storing the sampled data packets and a processor for identifying sources transmitting data packets to and from the network in excess of a predetermined rate.

17. The system according to claim 16 wherein the monitoring member is configured to exclude data packets transmitted to and from the network by the identified source.

18. The system according to claim 17 wherein the memory is configured to maintain a count of the number of data packets transmitted from any source to and from the network.

19. In combination with a firewall, a computer running a plurality of packet daemons for monitoring the data ports of a network, each data port monitored by a separate packet daemon, and each packet daemon configured to identify any source that transmits data packets through its data port in excess of a predetermined rate resulting in the firewall excluding the data packets from the identified source.

20. The computer of claim 19 further comprising a memory for storing the data packet count of transmitted data packets from any source.